

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:
INFORMATION ASSOCIATED WITH

HPWIDEN69@GMAIL.COM

THAT IS STORED AT PREMISES
CONTROLLED BY:
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Magistrate No. *18-1213*

[UNDER SEAL]

AFFIDAVIT

I, Kiera Fludd, being duly sworn, do hereby state and depose as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a United States Postal Inspector with the United States Postal Inspection Service (USPIS) and have been so employed since July of 2017. I am currently assigned to the Fraud Team for the Pittsburgh Field Office. Before being assigned to the Pittsburgh Field Office, I attended the USPIS's 12-week Postal Inspector training at the Career Development Unit in Potomac, Maryland. By virtue of my USPIS employment, I perform and have performed a variety of investigative tasks, to include assisting other agents in the execution of search and seizure warrants and the collection of evidence including computer/electronic related evidence. I have gained experience in and received training in general law enforcement practices and criminal investigations, including in interviewing and interrogation techniques, in the execution of federal search and seizure warrants, and in the identification and collection of computer-related evidence. I am a law enforcement officer charged with investigating possible violations of federal criminal

laws, including Title 18, United States Code, Sections 1001 (False statements) and 1512(c) (“Whoever corruptly . . . obstructs, influences, or impedes any official proceeding”).

2. I make this affidavit in support of an application for the issuance of a search warrant, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to search certain Google Inc. ("Google") Gmail email accounts for evidence concerning the violation of Title 18, United States Code, Sections 1001 and 1512(c).

3. The information to be searched is the Gmail email account **hpwiden69@gmail.com** (hereinafter the “TARGET ACCOUNT”), which is stored at premises owned, maintained, controlled, or operated by Google. The TARGET ACCOUNT is stored at premises owned, maintained, controlled, or operated by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, as further described in Attachment A, which is attached hereto and incorporated by reference. The warrant will require Google, a provider of electronic communications services and/or remote computer services, to disclose to the government the records, contents of communications, and other information in its possession as specified in Attachment A and in Section I of Attachment B, which are attached hereto and incorporated by reference. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to seize any evidence concerning a potentially fraudulent email as well as the identity and whereabouts of the person who used the accounts, as further described in Section II of Attachment B.

4. The information contained in this affidavit is based on my personal knowledge and observations, information and knowledge obtained from witnesses and other law enforcement personnel, information from computer experts, my review of documents, records, and other

evidence obtained during the investigation, information available on the Internet, and information gained through my training and experience. Since this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact I know regarding this investigation.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. 1001 (Making false statements) and 1512(c) (Corruptly influence an official proceeding) have been committed by the person(s) who have control of and/or access to the TARGET ACCOUNT. There is also probable cause to search the information described in Attachment A for evidence of these crimes and the identity of the individual(s) involved with these crimes as further described in Attachment B.

6. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

8. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

9. This affidavit concerns the falsification of an email/statement provided to a federal law enforcement agent in an effort to appear that the law enforcement agent withheld *Brady* evidence in order to obstruct/impede/influence the results of a trial and/or to influence the sentencing.

Subject Under Investigation

10. ATTICUS SLITER-MATIAS is the subject of this investigation as the individual who sent a falsified e-mail to a federal law enforcement officer in an effort to appear that the law enforcement agent withheld *Brady* evidence.

11. ATTICUS SLITER-MATIAS is a 27-year old Caucasian male who resides at 13781 Cedar Road, Apartment 205, South Euclid, OH 44118.

12. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that ATTICUS SLITER-MATIAS violated Title 18, United States Code, Sections 1001 and 1512(c) and that there exists evidence of these violations within the contents of the TARGET ACCOUNT.

Pending Case Against SLITER-MATIAS

13. On February 7, 2017, a federal grand jury sitting in the Western District of Pennsylvania returned a 2-count Indictment against ATTICUS SLITER-MATIAS in violation of 18 U.S.C. § 1341. The case was docketed at 17-34.

14. The Indictment set forth that from, in and around June 2015, and continuing thereafter to on or about July 5, 2016, ATTICUS SLITER-MATIAS devised or intended to devise a scheme to defraud individuals, and obtain money by means of materially false and fraudulent pretenses, representation, and promises, well knowing at the time that the pretenses,

representations, and promises were false and fraudulent when made.

15. From May 23, 2018 to May 31, 2018, a jury trial on the above Indictment was held in front of visiting District Court Judge Bill R. Wilson. The evidence presented at trial established that ATTICUS SLITER-MATIAS engaged in an eBay fraud scheme. From June 2015 to July 5, 2016, ATTICUS SLITER-MATIAS opened numerous fraudulent eBay and PayPal accounts that were registered with different false names, different Gmail email addresses and different prepaid gift cards. ATTICUS SLITER-MATIAS would advertise electronic devices for sale on these fraudulent eBay account that he had created. ATTICUS SLITER-MATIAS had no intention of delivering the electronic devices. When a buyer (victim) purchased the electronic device they paid through the eBay platform through PayPal or some other payment method. ATTICUS SLITER-MATIAS would engage in behavior that would release the funds from PayPal. For instance, SLITER-MATIAS often uploaded the tracking number for an empty package that he would send to a business in the same zip code of the victim (i.e., he would trick PayPal into believing this tracking number was associated with a package destined for the victim). Once the funds were released, SLITER-MATIAS would use the stolen funds to purchase gold, silver, or other items that would be delivered to his and his mother's UPS store box. To prevent the victim from filing a complaint prior to the release of the funds, SLITER-MATIAS would send the victim empty packages that was paid for with his credit card. SLITER-MATIAS would send the victims the tracking number for this empty package so the victims believed that their purchased electronic device was being delivered. When the victims received an empty envelope, they would file a complaint with eBay or PayPal, but, by then, SLITER-MATIAS would have used the victim's money to purchase the gold, silver, or other items.

16. The United States presented evidence that the SLITER-MATIAS used 161 fraudulent eBay accounts to engage in this scheme from June 2015 to July 2016. In addition, the United States presented evidence of spreadsheets that were recovered from SLITER-MATIAS's electronic devices that contained hundreds of eBay accounts that SLITER-MATIAS had created (there were far more accounts created prior to June 2015). These eBay accounts were registered with fraudulent Gmail email addresses. These spreadsheets contained records concerning these eBay and Gmail accounts.

17. At the trial, SLITER-MATIAS testified. He admitted to creating these eBay, PayPal, and Gmail accounts. He admitted that he sent the victims empty packages, and records were produced that the victim's monies were converted to gold and silver that was delivered to his UPS mailbox. Nevertheless, SLITER-MATIAS's defense was that he sold these eBay accounts to other individuals and that he was not responsible for the advertisement. He explained that these accounts were part of an underground market for "eBay stealth accounts" so legitimate vendors can bypass eBay's selling restrictions. He claimed he was unaware of the fraudulent advertisements even though his detailed spreadsheets maintained a ledger containing the victims' names and the amount of money the victim paid for these advertised electronic devices.

18. On May 31, 2018, after an hour of deliberation, the jury found ATTICUS SLITER-MATIAS guilty on both counts of mail fraud.

19. Sentencing is currently scheduled for October 1, 2018.

PROBABLE CAUSE

20. During the investigative stage, the case agent, Postal Inspector Lindsay Weckerly, attempted to contact potential victims of the Defendant's eBay accounts. In reviewing the

different eBay and PayPal accounts, Postal Inspector Weckerly learned that an eBay account in the name of Paul Widen had purchased an item from one of SLITER-MATIAS' fraudulent eBay accounts. Postal Inspector Weckerly also learned that there was a SLITER-MATIAS created eBay account in the name of Paul Widen.

21. According to the eBay records, the email address for the real Paul Widen account was hpwiden@msn.com. The email address for the SLITER-MATIAS created Paul Widen eBay account was hpwiden69@gmail.com.

22. The email address hpwiden69@gmail.com is an email account that appears on the spreadsheets that were recovered from SLITER-MATIAS' electronic devices and admitted in evidence. According to these spreadsheets, the hpwiden69@gmail.com email address was associated with eBay account that had the username HPwiden692 that SLITER-MATIAS created.

23. On December 21, 2015, Postal Inspector Weckerly attempted to contact the real Paul Widen by telephone and spoke to Paul Widen's wife. Unfortunately, Mr. Widen was unavailable. Having failed to reach Mr. Widen by telephone, Postal Inspector Weckerly attempted to contact Mr. Widen by email.

24. On December 23, 2015, Postal Inspector Weckerly sent an email to Paul Widen inquiring about the purchases from his eBay account. However, Postal Inspector Weckerly accidentally sent the email to hpwiden69@gmail.com (i.e., the fraudulent email accounts) instead of Mr. Widen's actual email account of hpwiden@msn.com.

25. Postal Inspector Weckerly never received a response to her email from hpwiden69@gmail.com.

26. On September 17, 2018 (two weeks before SLITER-MATIAS' Sentencing), for the first time, Postal Inspector Weckerly received a response from the email address **hpwiden69@gmail.com**. However, the email response contained within it an email chain that included an email purporting that **hpwiden69@gmail.com** responded to Postal Inspector Weckerly's email on February 7, 2016. This purported February 7, 2016 response asserted that the eBay/PayPal account was purchased from an "eBay Stealth" provider, which would have supported the Defendant's testimony at trial. The purported February 7, 2016 response stated the following:

This is an old account that is no longer actively being monitored. This account was purchased from an "eBay Stealth" provider online a while back for sales before Paypal arbitrarily shut it down. I don't know exactly what business activity you are referring to specifically since you didn't mention whom. We have multiple eBay and Paypal accounts which spread out sales under DBAs. Possible payments regarding that amount that we would've sent through this one were probably for software or product sourcing. Thank you.

27. The content for the September 17, 2018 email provided the following:

Sorry for the delay, health issues. There is a vendor that requested some documentation from us very recently. I exported and sent to him the original email reply that I wrote to you on 02/07/2016 indicating the ebay/paypal account was purchased and its current status. He seemed rather interested in your email. We never received a reply from you.

28. The clear indication of these emails is to suggest that Postal Inspector Weckerly did not disclose the purported February 7, 2016 email, which would have been *Brady* evidence, prior to the trial.

29. Postal Inspector Weckerly reviewed her email account and confirmed that she did

not receive this purported February 7, 2016 email. Moreover, on September 19, 2018, the Corporate Information Security Office of the United States Postal Service conducted an eDiscovery data search on Postal Inspector Weckerly's email account for any and all communications with hpwiden69@gmail.com. Based on communication with the specialist who performed the search, your Affiant knows that the results of this search would provide any and all e-mails sent to or received from hpwiden69@gmail.com, including any email communications that Postal Inspector Weckerly may have deleted. The Corporate Information Security Office was able to search Postal Inspector Weckerly's emails from November 1, 2015 to September 16, 2018. During this time period there was no emails received from hpwiden69@gmail.com and only one email sent to hpwiden69@gmail.com, which was Postal Inspector Weckerly's original email dated December 23, 2015. Thus, the Corporate Information Security Office was able to confirm that Postal Inspector Weckerly never received this purported February 7, 2016 email from hpwiden69@gmail.com.

30. Furthermore, on September 18, 2018, Postal Inspector Weckerly telephonically contacted the real Paul Widen, who confirmed that he had purchased Adobe software from one of ATTICUS SLITER-MATIAS' eBay accounts in 2012. According to Mr. Widen, he recalled this purchase because, after a period of time, he was contacted by Adobe and told the product key for the software was no longer valid. He further confirmed that he never received an email from Postal Inspector Weckerly on December 23, 2015, and that he never used or had access to the email address hpwiden69@gmail.com.

31. Based on my knowledge, training, and experience, your Affiant is aware that individuals can send emails so that it appears that there were additional, fictitious emails in the chain of communication.

32. Based on my training and experience, your Affiant knows that emails sent by a Gmail account is stored in the email accounts' "mail box" on Google servers until the account user deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google servers for a certain period of time. Thus, access to hpwiden69@gmail.com's mail box may provide evidence that the purported February 7, 2016 email was never sent.

33. In my training and experience, emails in email accounts often contain evidence of the identification of the creator and/or user of the account, including, but not limited to personal email correspondences, emails forwarded to personal email accounts, email attachments, and email addresses of correspondents who can later identify the user of the email account. Thus, based upon my knowledge, training, and experience, your Affiant is aware that information stored by Google and associated with the email account hpwiden69@gmail.com may contain emails and IP log records as to the true identity of the individual who controls the email account.

34. Based on the foregoing, there is probable cause to believe that the Google email account hpwiden69@gmail.com contains evidence of crimes in violation of 18 U.S.C. § 1001 & 1502(c) and/or evidence of the true identity of the person who committed such crimes.

35. The items to be seized from the TARGET ACCOUNT include any and all evidence that the purported February 7, 2016 email was never sent and/or the true identity and whereabouts of the person(s) who used the TARGET ACCOUNT on September 17, 2018, as more fully

described in Attachment B to the proposed search warrant, which is incorporated herein by reference.

BACKGROUND CONCERNING EMAIL

36. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

38. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other

identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

39. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

40. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result

of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account

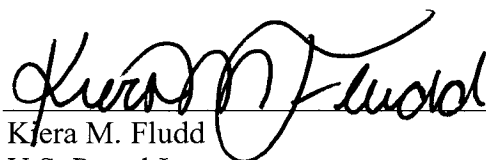
owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

42. Based on the forgoing, your Affiant requests that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

The above information is true and correct to the best of my knowledge, information and belief.

Respectfully submitted,



Kiera M. Fludd
U.S. Postal Inspector
United States Postal Inspection Service

Subscribed and sworn to before me
this 21st day of September, 2018



MAUREEN P. KELLY
Chief United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Gmail email account **hpwiden69@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, Inc. ("Google"), which information is stored at premises owned, maintained, controlled, or operated by Google, a company that accepts service of legal process at Custodian of Records, Google, Inc., 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, photos or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U. S.C § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier given in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All content stored in, or on behalf of, the above listed email accounts.
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. The types of service utilized;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

g. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **5 days** of the issuance of this warrant.

II. Information to be seized by the government

a. All information described above in Section I, for each account or identifier listed on Attachment A, that constitutes contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1001 (Making false statements) and 1512(c) (“Whoever corruptly . . . obstructs, influences, or impedes any official proceeding”), or the identity of the person who sent the September 17, 2018 email to Postal Inspector Weckerly, including, but not limited to the following matters:

1. Any and all communications with Postal Inspector Weckerly;
2. Any and all evidence that the purported February 7, 2016 email to Postal Inspector Weckerly was never sent, including the lack of a sent email on or around that time period;
3. All records and correspondences relating to the true identity and whereabouts of the user of the email account on or about September 17, 2018;
4. The identity of the person(s) who used the email account on September 17, 2018, including records that help reveal the whereabouts of such person(s);

5. Photographs, videos, and calendar entries identifying the physical characteristics of the true identity and whereabouts the person who created and/or used the account;

6. Address book and/or contact and buddy lists of individuals who can assist in identifying the true identity and whereabouts of the person who created and/or used the account;

7. All contact and personal identifying information, including subscriber's name, subscriber's birth date, subscriber's physical address, subscriber's alternative email addresses, subscriber's telephone number and other identifiers;

8. Personal email correspondences, e-mails forwarded to a personal email account, email attachments, email addresses of correspondents who can later identify the user of the email account;

9. All log records showing when the account was accessed;

10. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

11. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

12. Records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, the log-in IP addresses associated with session times and dates, the methods of connecting, and the log files; and

13. The means and source of payment.